REMARKS

Claims 1-22 are pending in this application, and claims 1 and 13 are amended herein. Based on the discussions during the telephonic Interview of August 2, 2006, the Amendments presented above, and the following remarks, Applicants respectfully request reconsideration and allowance of this application.

Claims 1-8, 10-20, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,084,969 to Wright et al. in view of U.S. Patent No. 6,073,237 to Ellison. In addition, claims 9 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright and Ellison, in further view of the Irish Times article noted by the Examiner. However, Wright, Ellison, and the Irish Times article, taken alone or in combination, fail to disclose, teach or suggest all of the features recited in the claims.

For example, independent claim 1 recites a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of generating a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document, encrypting the original document with the session key to create an encrypted document, generating a proxy key based on a public key corresponding to the selected recipient; and applying the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein *the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation*.

As was discussed in the Interview, Wright teaches a well-known decryption / re-encryption method including "using a pager proxy to carry out decryption of a message encrypted by a session key and received from the sending pager, and to have the pager proxy generate a new session key for re-encryption of the message transmitted to the receiving pager. . ." (Col. 4, line 65-Col. 5, line 2). According to Wright, the encrypted message does not remain encrypted during application of a new key to the message. In particular, Wright teaches, in Col. 13, line 45, to Col. 14, line 30, the steps of encrypting a message with a session key (step 170), transmitting the encrypted message to the pager proxy (see FIG. 8),

decrypting the message using the session key (step 240), generating a new session key (step 300), and re-encrypting the message using the new session key (step 310). It is noted that the Examiner also points to column 14, lines 61-67 of Wright et al., which state that "although the preferred embodiment of the invention has the pager proxy re-package the message by first decrypting it, and then re-encrypting it using a new session key, it is also within the scope of the invention to have the pager proxy decrypt only the session key and re-encrypt the same session key using the public key or shared secret key of the destination pager." The Examiner further points to Col. 13, lines 2-15, of Wright and suggests that Wright teaches a method of encrypting a message and the subsequently further encrypting the message with a second encryption for the message without decrypting the message during the transformation. However, neither of these portions of Wright discloses applying a public proxy key to an encrypted message to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and the available public key information, and wherein the encrypted message remains in an encrypted state while being transformed into the transformed message and is not decrypted to the original message and re-encrypted at any point during the transformation, as is recited in the claims. Accordingly, Wright fails to disclose, suggest, or render obvious the noted features recited in the claims.

Similarly, Ellison is applied based on its disclosure of a 'wallet,' which is an electronic version of money held by a user is protected in part by a private key known only to the user. The private key is kept secret since the key is part of wallet data which is encrypted and stored in a computer. (See Col. 1, lines 20-26). In addition, the Irish Times article is applied based on its mentioning of the Cramer-Shoup method. However, Ellison and the Irish Times article fail to cure the deficiencies in Wright noted above.

In contrast to the teachings of Wright, Ellison, and the Irish Times article, the Examiner's attention is respectfully directed to FIGS. 5,8-10, and 13, and related discussions on pages 21, 29-34, and 39-43 of the specification, which clearly supports the claims. FIG. 5, and page 21, lines 5-18, of the Specification, clearly disclose the broad concept of the invention, which comprises four generic steps: message encryption, proxy key generation, proxy transformation, and message decryption. These steps are outlined below, with

reference to FIG. 5.

> 1. Message encryption E: The encryptor generates an encrypted message using grantor's encryption key and delivers it to the grantor (step 510).
>
> 2. Proxy generation π: To delegate the decryption right to the grantee, the grantor generates a proxy key π as a commitment token that allows the grantee to decrypt the message encrypted for the grantor (step 512).
>
> 3. Proxy transformation Π: When necessary, the facilitator performs a proxy transformation Π, possibly using the proxy key π, to convert the message encrypted for the grantor to a message encrypted for the grantee (step 514).
>
> 4. Message decryption D: Upon receiving the transformed message and possibly the proxy key π, the grantee decrypts the message (step 516).

The transformation step recited in the claims is more specifically described with reference to the Blaze and Straus encryption scheme in FIG. 8, and on pages 29-30 of the Specification. In particular, lines 7-21 on page 29 provide that:

> Turning now to Figure 8 in more detail, given a message m that needs to be sent to a grantor A with public key a, the message m is encrypted by uniformly choosing a random number $k \in \mathbf{Z}^*_{p-1}$ (step 810) and calculating a pair of numbers (r, s) representing the encrypted message (step 812) as follows:
>
> $$r = mg^k \pmod{p} \text{ and } s = a^k \pmod{p}.$$
>
> To delegate the decryption right to a grantee B, the grantor A creates a proxy key π by obtaining B's private decryption key b (step 814) and computing $\pi = a^{-1}b \pmod{p-1}$ (step 816), where a^{-1} is the inverse of the private key a of A modulo p-1. The proxy key π can be made public.
>
> To use the proxy key π to convert a message (r, s) encrypted for A to a message encrypted for B, the facilitator (not necessarily A, since the proxy key π is public) computes $s' = s^{\pi} \pmod{p}$ (step 818). The pair (r, s') represents the transformed encrypted message, which can then be transmitted to B.
>
> To decrypt the transformed message, B computes $m = r(s'^{a^{-1}})^{-1} \pmod{p}$ (step 820), where b is B's private key and b^{-1} is the inverse of b modulo p-1.

Here, the transformation of the encrypted message occurs in step 818 when the proxy key is applied to the encrypted message (r,s), encrypted for A, to transform the encrypted message into a transformed message (r,s'), encrypted for B. Contrary to the teachings of

Wright, it is possible for an untrusted facilitator or server to perform the proxy transformation. (Pg. 30, lines 9-10).

Similarly, FIG. 9, and related text on page 31 of the Specification, illustrates the transformation step recited in the claims with reference to the ElGamal encryption scheme. In particular, lines 12-22 on page 31 provide:

> Referring now to Figure 9, given a message m that needs to be sent to a grantor A with public key α, the message m is encrypted by uniformly choosing a random number $k \in \mathbf{Z}^*_{p-1}$ (step 910) and calculating a pair of numbers (r, s) representing the encrypted message (step 912) as follows:
>
> $$r = g^k \pmod{p} \text{ and } s = m\alpha^k \pmod{p}.$$
>
> To delegate the decryption right to a grantee B, grantor A creates a proxy key π by obtaining B's authentic decryption key b (step 914) and calculating $\pi = r^{b-a} \pmod{p}$ (step 916).
>
> The message is transformed from (r, s) to (r, s') by calculating $s' = s\pi \pmod{p}$ (step 918). The message m is then decrypted by B from (r, s') by computing $m = s'(r^b)^{-1} \pmod{p}$ (step 920).

Here, the transformation of the encrypted message (r,s) to transformed message (r,s') occurs in step 918 when the proxy key is applied to the encrypted message (r,s) to transform the encrypted message into the transformed message (r,s').

In addition, FIG. 10, and related text on pages 32-33 of the Specification, describes another embodiment of the invention utilizing the transformation step recited in the claims. In particular, line 30, on page 32, to line 9, on page 32, provides:

As shown in Figure 10, given a message m that needs to be sent to a grantor A with public key a, the message m is encrypted by uniformly choosing a random number $k \in \mathbf{Z}^*_{p-1}$ (step 1010) and calculating a pair of numbers (r, s) representing the encrypted message (step 1012) as follows:

$$r = mg^k \pmod{p} \text{ and } s = a^r \pmod{p}.$$

To delegate the decryption right to a grantee B, grantor A creates a proxy key π by obtaining B's authentic decryption key b (step 1014) and calculating $\pi = (s^{a^{-1}})^{b-a} \pmod{p}$ (step 1016), where a^{-1} is the inverse of a modulo p-1.

The message is transformed from (r, s) to (r, s') by calculating $s' = s\pi \pmod{p}$ (step 1018). The message m is then decrypted by B from (r, s') by computing $m = r(s'^{b^{-1}})^{-1} \pmod{p}$ (step 1020), where b^{-1} is the inverse of b modulo p-1.

Here, the transformation of the encrypted message (r,s) to transformed message (r,s') occurs in step 1018 when the proxy key is applied to the encrypted message (r,s) to transform the encrypted message into the transformed message (r,s').

Accordingly, the methods recited in the claims including the application of the public proxy key to the encrypted message to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and the available public key information, and wherein the encrypted message remains in an encrypted state while being transformed into the transformed message and is not decrypted to the original message and re-encrypted at any point during the transformation, is clearly and specifically supported by the Specification as is described above.

Accordingly, for at least the reasons described above, Wright, Ellison, and the Irish Times article, alone or in combination, fail to disclose or render obvious each and every element recited in independent claims 1 and 13, including the steps of generating a proxy key and applying the public proxy key as recited by claims 1 and 13. Thus, Applicants respectfully submit that Wright, Ellison, and the Irish Times article fail to render claims 1 and 13 obvious under 35 U.S.C. § 103(a), and respectfully request that this rejection be reconsidered and withdrawn. Dependent claims 2-12, 14-22 are allowable on the basis of

their dependency on claims 1 and 15, as well as on their own merits.

The present amendment is submitted in accordance with the provisions of 37 C.F.R. §1.116, which after Final Rejection permits entry of amendments placing the claims in better form for consideration on appeal. As the present amendment is believed to overcome outstanding rejections under 35 U.S.C. § 103, the present amendment places the application in better form for consideration on appeal. It is therefore respectfully requested that 37 C.F.R. §1.116 be liberally construed, and that the present amendment be entered.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution. **Except** for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a **CONSTRUCTIVE PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

NIXON PEABODY, LLP

Date: August 7, 2006

/Stephen M. Hertzler, Reg. # 58,247/
Stephen M. Hertzler

Customer No.: 22204
NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, D.C. 20004-2128
(202) 585-8000